

Performance of Lattice Coset Codes on Universal Software Radio Peripherals

Jinlong Lu, J. Harshan, and Frédérique Oggier

Division of Mathematical Sciences,

School of Physical and Mathematical Sciences,

Nanyang Technological University, Singapore

{kerin_lu, jharshan, frederique}@ntu.edu.sg

Abstract

We consider an experimental setup of three Universal Software Radio Peripherals (USRPs) that implement a wiretap channel, two USRPs are the legitimate players Alice and Bob, while the third USRP is the eavesdropper, whose position we vary to evaluate information leakage. The experimented channels are close to slow fading channels, and coset coding of lattice constellations is used for transmission, allowing to introduce controlled randomness at the transmitter. Simulation and measurement results show to which extent coset coding can provide confidentiality, as a function of Eve's position, and the amount of randomness used.

Index Terms

Physical-layer security, Coset coding, Eavesdropping, Lattice codes, USRP.

This work was funded in part by the Singapore National Research Foundation under Research Grant NRF-RF2009-07 and under Research grant NRF/2014/MDT14.

I. INTRODUCTION

We consider a wiretap channel, comprising a legitimate transmitter, Alice, and two receivers: a legitimate one, Bob, and a passive adversary, Eve. For the legitimate users Alice and Bob, both reliable and confidential transmission needs to be achieved, while Eve is trying to eavesdrop the communication. This is done through wiretap coding. Alice encodes her secret s into a codeword x belonging to a code \mathcal{C} , and x is then sent through the wiretap channel to Bob and Eve, which respectively receives y_B and y_E . What distinguishes wiretap coding from standard coding is the constraint on confidentiality, which should be obtained without invoking cryptographic means: confidentiality is obtained by a suitable injection of controlled randomness mixed with an appropriate coding strategy at the transmitter, which enables Bob to receive his message with high probability, while confusing the eavesdropper to the point of making her knowledge of the secret message negligible. This is formally expressed by saying that the mutual information between what Eve receives and the secret is zero:

$$I(s; y_E) = H(s) - H(s|y_E) = 0 \quad (1)$$

or equivalently, that the entropy $H(s|y_E)$ of the secret knowing the received message at the eavesdropper is the same as the entropy of the secret.

Wiretap coding necessarily requires the channel from Alice to Bob to be different from that from Alice to Eve. What “different” means, as well as wiretap coding strategies, depend on the channel model, e.g., discrete memoryless, additive white Gaussian, Rayleigh fading, or multiple-input multiple output (MIMO), to name a few popular models. We refer the readers to [1] and [2] for a survey of information theoretic results and respective coding strategies for wiretap channels, and to [3]-[5] for application of practical codes on wiretap channels.

In all cases, the channel assumptions, in particular regarding the eavesdropper’s channel, are critical, since the confidentiality analysis relies on them. This is the case for wiretap coding, but also for any other schemes whose security relies on channel noise, such as secret key generation.

The goal of this paper is to study wiretap coding from an experimental view point using a USRP testbed comprising three USRPs, one for each of the three players, Alice, Bob and Eve. The channels between Alice and Bob, and Alice and Eve respectively, are close to slow fading channels, whose SNRs and noise are given by the experimental settings. Transmission is done using signal constellations from lattices, which are transmitted using coset coding as explained in Section II, to introduce controlled randomness (for that reason, we will use the term “coset coding” rather than wiretap coding in the rest of the paper). The positions of Alice and Bob are kept fixed, while we vary the position of Eve to analyze her received signal, and how much information is leaked depending on both her position and the coding scheme used.

We present both simulations and experimental results that consistently show how coset coding does provide confusion at the eavesdropper, with entropy (see Subsection II-B) and decoding error as metrics, using an optimal decoder for Eve, as proven in Subsection II-C. Extensive results are provided in Section III and Section IV, to compare coset coding versus conventional coding, but also different coding schemes using lattice constellation of different dimensions, different amounts of randomness and different positions for Eve. Experiments were realized by transmitting “the cameraman image” (see Fig. 4), which furthermore allows a visualization of the effect of coset coding (see Fig. 12).

We believe that this type of experimental work is critical to the development of physical layer security, since it gives an insight of how practical a security scheme such as coset coding behaves in practice, without having to rely on channel assumptions. Another work with the same philosophy was done for key generation in [6], where the authors investigate the role of the eavesdropper’s statistics when actually implementing a secret-key generation system over a wireless channel. This is done via a software-defined radio testbed, where the channel gains are measured. The experimental setup shows a 20% loss in secret-key rate with respect to theoretical bounds.

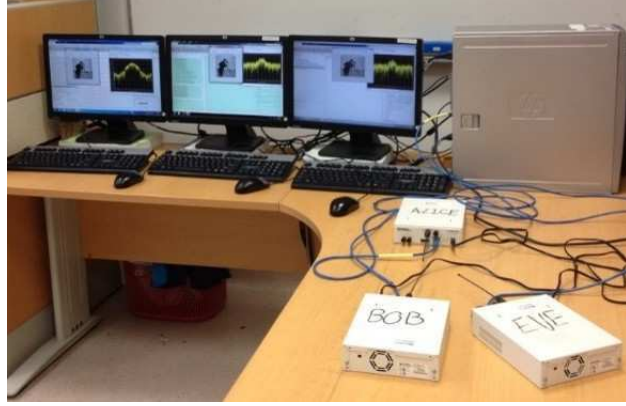


Fig. 1. USRP testbed, comprising three USRPs: a transmitter (Alice) and two receivers (Bob and Eve).

II. COSET ENCODING OF LATTICE CODES

We consider a wiretap testbed formed by three USRPs, as shown on Fig. 1. One USRP plays the role of the legitimate transmitter Alice, while the other two USRPs are the receivers, Bob and Eve.

This wiretap channel is modeled by

$$\mathbf{y}_B = h_B \mathbf{x} + \mathbf{n}_B \quad (2)$$

$$\mathbf{y}_E = h_E \mathbf{x} + \mathbf{n}_E \quad (3)$$

where $h_B, h_E \in \mathbb{C}$ are the respective channel gains, $\mathbf{x} \in \mathbb{C}^{L/2}$ is the transmitted message (L is the real dimension, an even number), and $\mathbf{n}_B, \mathbf{n}_E$ are the respective channel noises at Bob and Eve, distributed as circularly symmetric complex Gaussian, denoted by as $\mathcal{CN}(\mathbf{0}, \sigma^2 \mathbf{I}_{L/2})$.

To transmit over this complex channel, we consider lattice coding. A real lattice Λ of dimension L is a discrete set of points in \mathbb{R}^L generated as integral linear combinations of a set of L linearly independent vectors in \mathbb{R}^L . For actual data transmission, a finite constellation of the lattice is chosen. For example, QAM constellations are obtained by taking a finite subset of the lattice \mathbb{Z}^L . When L is even, a real lattice can be used for transmission over a complex channel of dimension

$L/2$. The role of a lattice encoder is to map a bit string to a lattice point. However for wiretap coding, we use instead lattice coset coding, which allows us to introduce randomness.

A. Lattice Coset Coding

At the transmitter, we implement a lattice coset encoder. A lattice coset encoder requires two nested lattices $\Lambda_E \subset \Lambda_B$, and a partition of Λ_B as a union of cosets of Λ_E :

$$\Lambda_B = \cup_{\mathbf{s} \in \Lambda_B/\Lambda_E} (\mathbf{s} + \Lambda_E) \quad (4)$$

where \mathbf{s} is a coset representative. In Fig. 2, a lattice Λ_B is shown as the union of the lattice $\Lambda_E = 2\mathbb{Z}^2$ and its coset $2\mathbb{Z}^2 + (1, 1)$.

In the context of wiretap coding, coset coding is used to create confusion by introducing controlled randomness. In this case, \mathbf{s} actually encodes the secret, while a vector \mathbf{r} is chosen randomly inside Λ_E , to obtain $\mathbf{x} = \mathbf{s} + \mathbf{r}$. We use the index B in Λ_B to indicate that this lattice is used for transmission to Bob, while Λ_E is the lattice meant to create confusion at Eve's end.

A partition of Λ_B as a union of cosets of a sublattice Λ_E can be obtained using the so-called Construction A [7]. Let $\rho : \mathbb{Z}^L \rightarrow \{0, 1\}^L$ denote the componentwise reduction modulo 2, which maps an integral vector to a binary one. In $\{0, 1\}^L$, choose a binary linear code C of length L and dimension k . Then we take for Λ_B the lattice $\rho^{-1}(C) = 2\mathbb{Z}^L + C$ (possibly scaled), and thus $\Lambda_E = 2\mathbb{Z}^L$. Codewords from C are the coset representatives. The lattice on Fig. 2 is called D_2 , and is actually obtained using Construction A and the repetition code $C = \{(0, 0), (1, 1)\}$:

$$D_2 = 2\mathbb{Z}^2 + C = (2\mathbb{Z}^2 + (0, 0)) \cup (2\mathbb{Z}^2 + (1, 1)).$$

Table I lists different constructions A of lattices that we use.

For an infinite lattice, the vector \mathbf{r} introduced for randomness is chosen according to the uniform distribution. To perform experiments, finite constellations are carved from lattices, by taking lattice points in the hypercube $\{0, 1, 2, \dots, M-1\}^L$, and we keep the choice of a uniform

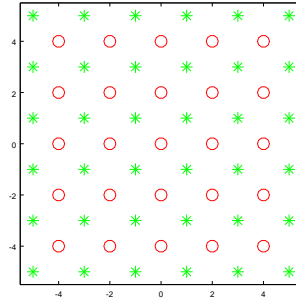


Fig. 2. The lattice D_2 obtained via Construction A. The circles are used for the lattice $2\mathbb{Z}^2$, and the stars for the coset $2\mathbb{Z}^2 + (1, 1)$.

Λ	L	C
\mathbb{Z}^2	2	$\{00, 01, 10, 11\}$
D_2	2	$\{00, 11\}$
D_4	4	$(4, 3, 2)$ parity check
$\sqrt{2}E_8$	8	$(8, 4, 4)$ Reed-Müller

TABLE I

LATTICES VIA CONSTRUCTION A: $\Lambda = 2\mathbb{Z}^L + C$.

distribution for the randomness used (a possibility for further experiments could be to use instead the distribution proposed in [8]).

In what follows, we use the terminology *standard* or *conventional encoding* to refer to lattice coding (say data points are mapped to points in D_2 or E_8) without use of randomness, in contrast to *coset encoding* which introduces randomness as explained above.

B. Conditional Entropy at Eve

Recall from (1) that confidentiality is measured by

$$I(\mathbf{s}; \mathbf{y}_E) = H(\mathbf{s}) - H(\mathbf{s}|\mathbf{y}_E),$$

and coset encoding should ensure that $I(\mathbf{s}; \mathbf{y}_E) = 0$. Ideally, we thus would want $H(\mathbf{s}|\mathbf{y}_E) = H(\mathbf{s})$. With this objective in mind, it is interesting to observe how close are the values of $H(\mathbf{s}|\mathbf{y}_E)$ and $H(\mathbf{s})$, that arise from the coset encoding schemes in practice (to meet the confidentiality criterion). Since conditional entropy is independent of any specific decoder implementation at Eve, we use it to showcase the impact of coset encoding for creating confusion at Eve. To get a sense of the conditional entropy of coset encoding, we conducted Monte-Carlo simulations assuming a fixed channel gain h , for the following one-dimensional ($L = 1$) encoding schemes:

- Coset encoding using $\Lambda_E = 2\mathbb{Z}$ and $\Lambda_B = \mathbb{Z}$, where 1 bit of secret is mapped to a coset in $\mathbb{Z}/2\mathbb{Z}$, and the coset representative is chosen with 2 bits of randomness. If the coset $2\mathbb{Z}$ is chosen, then one of the elements in $\{0, 2, 4, 6\}$ is uniformly chosen as the representative. Similarly, one of the elements in $\{1, 3, 5, 7\}$ is uniformly chosen as the coset representative for the coset $2\mathbb{Z} + 1$.
- Conventional encoding using $\mathbb{Z}/2\mathbb{Z}$, where 1 bit of secret is deterministically mapped to the coset representatives $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$ (no randomness added).
- Conventional encoding using $\mathbb{Z}/8\mathbb{Z}$, where 3 bits of secret is deterministically mapped to the coset representatives $\mathbb{Z}/8\mathbb{Z} = \{0, 1, 2, \dots, 7\}$ (no randomness added).

To empirically compute conditional entropy, we transmitted a random ensemble of points from the above encoding schemes (after suitably scaling and shifting to keep their average transmit powers identical). Upon receiving the points \mathbf{y}_E in (3), we evaluated the conditional probability mass function $P(\mathbf{s}|\mathbf{y}_E = y)$, by looking at various \mathbf{s} values that result in a particular realization of \mathbf{y}_E , say $\mathbf{y}_E = y$. Then the conditional probability mass function on \mathbf{s} was obtained using frequency of occurrence of various realizations of \mathbf{s} . Note that experimentally, obtaining *multiple* realizations of \mathbf{s} that result in the same real number y is unlikely. As a result, we partitioned the real line into tiny bins so as to collect multiple realizations falling within the same bin. This allowed us to compute

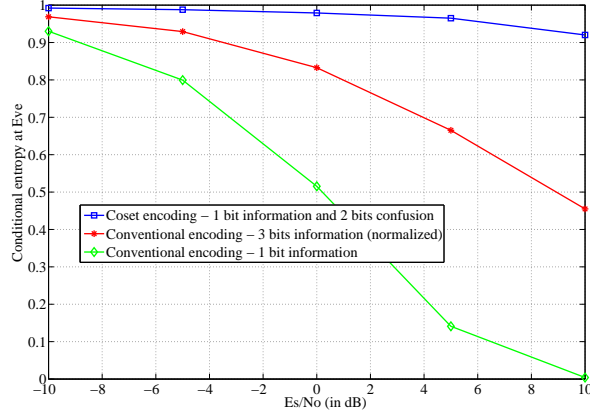


Fig. 3. Conditional entropy of various encoding schemes when measured at Eve. For the conventional scheme with 3 bits of information, conditional entropy is normalized to 1 bit for comparison purposes with other schemes. The plots show that coset encoding with 1 bit information and 2 bits of randomness results in conditional entropy close to 1 at Eve, thereby serving the confidentiality purpose.

$$H(\mathbf{s}|\mathbf{y}_E = y) = - \sum_j P(\mathbf{s} = j|\mathbf{y}_E = y) \log_2 P(\mathbf{s} = j|\mathbf{y}_E = y),$$

where j is used to denote different realizations of the secret \mathbf{s} . From the above expression, the conditional entropy numbers are obtained as

$$\tilde{H}(\mathbf{s}|\mathbf{y}_E) = - \sum_y P(y) H(\mathbf{s}|\mathbf{y}_E = y),$$

where $\tilde{H}(\mathbf{s}|\mathbf{y}_E)$ is an approximation to the standard entropy definition. The measured conditional entropy values for the three encoding schemes are given in Fig. 3. The plots show that the conditional entropy of coset encoding is close to 1 (which is the entropy of the secret), much higher than the other two conventional encoding schemes.

C. Suboptimal and Optimal Decoders

In the previous subsection, we studied the conditional entropy criterion, which is independent of the decoder employed at Eve. We next discuss relevant decoders for the coset encoding scheme. Consider a lattice code $\mathcal{C} \subset \mathbb{C}^{L/2}$ which can be partitioned into 2^k equally sized subsets as follows

$$\mathcal{C} = \mathcal{C}_0 \cup \mathcal{C}_1 \cup \dots \cup \mathcal{C}_{2^k-1},$$

where $|\mathcal{C}_0| = \dots = |\mathcal{C}_{2^k-1}|$ is a power of 2. At the encoder, based on k information bits, or rather k bits forming the secret \mathbf{s} in our case, one of the sets in $\{\mathcal{C}_0, \mathcal{C}_1, \dots, \mathcal{C}_{2^k-1}\}$ is chosen, and then a random codeword \mathbf{x} from the chosen set is transmitted. The choice of the random codeword is based on $\log_2(|\mathcal{C}_0|)$ random bits that are intended to create confusion at Eve. Specifically, if the l -th codeword in \mathcal{C}_j is chosen, for some $0 \leq j \leq 2^k - 1$, then \mathbf{x} will take the codeword denoted by $\mathbf{c}_j^{(l)}$. With that, the signal received at Eve is given by (3), namely (we drop the subscript E for the rest of this subsection to lighten the notation)

$$\mathbf{y} = h\mathbf{x} + \mathbf{n},$$

where h is the fading gain, \mathbf{n} is the AWGN distributed as circularly symmetric complex Gaussian, denoted by $\mathcal{CN}(\mathbf{0}, \sigma^2 \mathbf{I}_{L/2})$. When the average transmit power per channel use is P , the average Signal-to-noise ratio (SNR) is given by $\rho \triangleq \frac{P|h|^2}{\sigma^2}$.

The k -length bit sequence $\hat{\mathbf{s}}$ can be ML decoded as

$$\hat{\mathbf{s}} = \arg \max_{\{\mathcal{C}_j\}} P(\mathbf{x} \in \mathcal{C}_j | \mathbf{y}, h),$$

where $P(\cdot)$ denotes the conditional probability density function. By applying Bayes' rule, we

have

$$\begin{aligned}
\hat{\mathbf{s}} &= \arg \max_{\{\mathcal{C}_j\}} \frac{P(\mathbf{y}|h, \mathbf{x} \in \mathcal{C}_j)P(\mathbf{x} \in \mathcal{C}_j|h)}{P(\mathbf{y}|h)} \\
&= \arg \max_{\{\mathcal{C}_j\}} \sum_{l=1}^{|\mathcal{C}_j|} P(\mathbf{y}|\mathbf{x} = \mathbf{c}_j^{(l)}, h) \\
&= \arg \max_{\{\mathcal{C}_j\}} \sum_{l=1}^{|\mathcal{C}_j|} e^{-\rho \|\mathbf{y} - h\mathbf{c}_j^{(l)}\|^2}.
\end{aligned} \tag{5}$$

The second equality follows since $P(\mathbf{y}|h)$ is fixed and $P(\mathbf{x} \in \mathcal{C}_j|h)$ is a constant. The last equality follows from the fact that \mathbf{y} is Gaussian distributed when conditioned on \mathbf{x} and h . At high ρ values, (5) can be approximated as

$$\begin{aligned}
\hat{\mathbf{s}} &= \arg \max_{\{\mathcal{C}_j\}} e^{-\rho \|\mathbf{y} - h\mathbf{c}_j^{(l')}\|^2} \\
&= \arg \min_{\{\mathcal{C}_j\}} \|\mathbf{y} - \mathbf{c}_j^{(l')}\|^2,
\end{aligned} \tag{6}$$

where $\mathbf{c}_j^{(l')}$ is the closest codeword to \mathbf{y} (in Euclidean distance) among the members of \mathcal{C}_j . We refer to (5) and (6) as the Maximum Likelihood (ML) decoder and Minimum Distance (MD) decoder, respectively. In our preliminary work in [9], we have used the MD decoder to obtain experiment results on the error performance of coset encoding scheme. However, in this work, we employ the superior ML decoder to obtain the results. The use of (5) is imperative to showcase that despite the optimality of ML decoder, lattice code based coset encoding scheme results in higher confusion at Eve than the other conventional schemes.

Having introduced the optimal decoder for the coset encoding schemes, in the next section we use them to showcase how much secret can be extracted at Eve from \mathbf{y}_E .

III. EXPERIMENT SET UP USING USRPs

We illustrate the role and effectiveness of coset coding through experiments over a testbed, comprising National Instrument USRP-2920 devices (as shown on Fig. 1) to implement the wiretap channel consisting of Alice, Bob and Eve (all are single antenna devices). The experiments



Fig. 4. The *Cameraman* image transmitted from Alice to Bob. This image is extensively used as a test image in image processing research. This *Cameraman* image is transmitted in an unencrypted form so as to validate the effect of wiretap coset encoding.

were carried out by fixing the position of Alice and Bob while placing Eve at different positions. In particular, Bob is positioned at some fixed distance from Alice, referred to as Placement 1, whereas Eve is placed at five different distances, referred to as Placement 1, 2, 3, 4 and 5 (in the order of increasing distance).¹ Alice transmits the black-and-white image shown in Fig. 4 using either conventional coding or coset coding, whereas Eve attempts to recover this image at different positions. Using an image for the experiments gives a visualization of the effect of coset coding through the quality of the reconstructed image at Eve, i.e., more distortion of the recovered image implies more confusion at Eve. Since we have already discussed the benefits of coset encoding in terms of conditional entropy, we now present experiment results based on decoding error.

The system parameters of the experiment setup are listed in Table II and III. More details on the setup are available in [10]. Communication between the USRP devices takes place over

¹The use of 5 placements 1, 2, 3, 4 and 5 are only for the sake of introducing the setup. However, placements other than the above 5 have also been used to generate experiment results.

TABLE II

SYSTEM PARAMETERS FOR THE EXPERIMENTS. SDRu DENOTES SOFTWARE-DEFINED RADIO, AND LO DENOTES LOCAL OSCILLATOR.

Parameter	SDRu Transmitter	SDRu Receiver
Center Frequency (Hz)	2.42E+09	2.42E+09
LO offset(Hz)	0	0
Gain(dB)	18	31
Interpolation/ Decimation	500	500

TABLE III

PARAMETERS FOR RX/TX RAISED COSINE FILTER

Parameter	SDRu Transmitter/Receiver
Filter shape	square root
Rolloff Factor	0.5
Filter span in symbols	6
Input/Output samples per symbol	4
linear amplitude filter gain	1

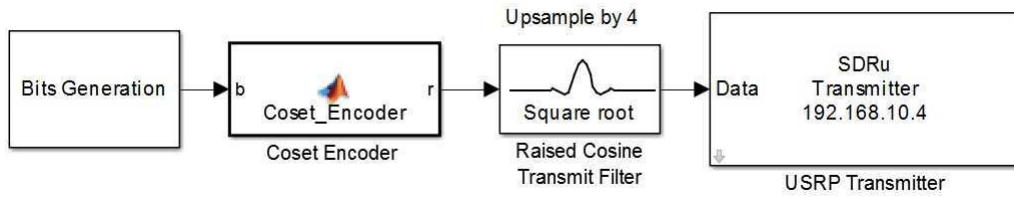


Fig. 5. Transmitter side baseband operations as implemented in our experiments on Matlab.

a sequence of frames where each frame constitutes $n = 100$ complex symbols in baseband representation. Among the 100 symbols, the first 13 symbols are QPSK modulated pilot symbols which are constructed by identically placing a 13-length binary Barker code sequence [11] on the in-phase and quadrature components. These pilot symbols are essential for the timing recovery and frame synchronization operations at the receiver. The rest of the 87 locations in the frame are allocated for data transmission. On the application level, the digital image is first broken down into a sequence of binary digits (around 64K bytes in size) and then these bits are communicated to Bob by spreading them over a sequence of frames. For the uncoded scheme, 87 binary symbols (from the set $\{0, 1\}$) are embedded into the frame, while for the coded schemes (both conventional and coset), these locations are loaded with uniformly chosen codewords from an underlying lattice code (carved from Λ_B , with $\Lambda_B \in \{D_2, D_4, E_8\}$). For the coded schemes, whenever the codewords do not fill the 87 symbols completely, the remainder locations are loaded with dummy symbols. Further, note that the codewords of the chosen lattice codes in \mathbb{Z} , D_2 , D_4 and E_8 have components with only non-negative real values. Hence, for implementation purpose, the symbols are appropriately shifted around the origin to reduce the average transmit power.

Our method to transmit the lattice codewords of \mathbb{Z} , D_2 , D_4 and E_8 is as follows. Irrespectively of whether the strategy is conventional encoding or coset encoding, for any $\mathbf{x} \in \{0, 1, \dots, M - 1\}^L$, where L is the dimension of the lattice, the transmitted codeword is of the form

$$\mathbf{x}_t = \frac{e^{-i\frac{\pi}{4}}}{\sqrt{E_{avg}}} \left(\mathbf{x} - \frac{M-1}{2} \right) \in \mathbb{C}^L, \quad (7)$$

where E_{avg} is the average energy of the shifted constellation $\{-\frac{M-1}{2}, -\frac{M-1}{2} + 1, \dots, \frac{M-1}{2} - 1, \frac{M-1}{2}\}$. Using the scale and the shift operation in (7), each component of \mathbf{x}_t takes value from a complex constellation with unit average energy. For the experiment, we use the carrier frequency compensation and timing recovery blocks that are tailor-made for QPSK signal sets [12]. Hence, to facilitate this reuse, the real lattice points are rotated by -45 degrees.

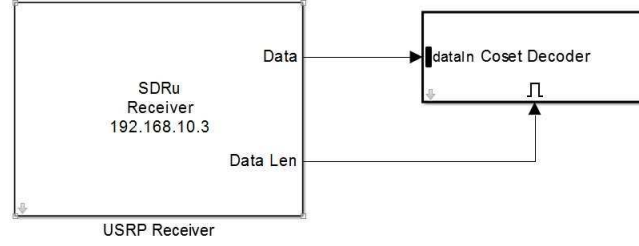


Fig. 6. Receiver block as implemented in our experiments on Matlab.

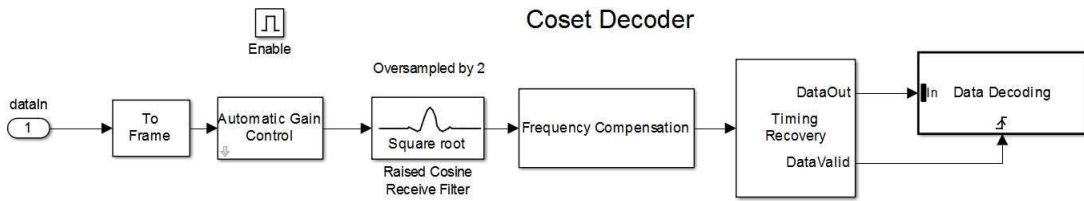


Fig. 7. Receiver side baseband operations as implemented in our experiments on Matlab.

Once a frame constituting Barker code symbols and lattice codewords $\{\mathbf{x}_t\}$ is generated, it is subsequently upsampled by 4 and then passed through a square-root raised cosine filter (with roll-off factor 0.5) for pulse shaping purpose (see Fig. 5 for the transmitter side baseband operations). Finally, the filtered samples are forwarded to the USRP device (with interpolation factor 500) for passband transmission.

A. Reception and Decoding

At the receiver, the passband signal is down-converted and appropriately sampled by the USRP hardware. Then these samples are forwarded to the simulink block (with decimation factor 500) for baseband processing (see Fig. 6 and 7 for the receiver side baseband operations).

A total of 4000 samples (equivalent to 10 received frames) are processed batch-wise in order to facilitate frame synchronization and timing recovery operations. For accurate synchronization,

the received samples are passed through an Automatic Gain Control (AGC) block before it is filtered using a square-root raised cosine receive filter (with identical parameters as that of the transmit filter). Subsequently, the filtered output is forwarded to the frequency compensation and timing recovery blocks. In the timing recovery block, the Barker code sequence is independently generated, using which the beginning of the received frames is detected through cross-correlation operations. Finally, the *aligned* frames are forwarded to the data decoding block (either conventional or coset), which assuming the frame synchronization is accurate, estimates the channel gain using the Barker code symbols on the first 13 locations. Since the AGC gain values may vary across successive frames, we use the estimated channel gain locally within a frame but not across frames. The received lattice codewords by Eve of the form

$$\mathbf{y}_E = h_E \mathbf{x}_t + \mathbf{n}_E$$

are extracted from the frame to carry out the decoding process. Here, the scalar h_E is the complex channel gain (for Eve) and $L \in \{1, 2, 4, 8\}$ is the block length of the lattice code. Using \mathbf{y}_E and \hat{h}_E (the estimated channel gain), the most likely transmitted lattice point is computed using the Maximum Likelihood (ML) decoder in (5).

In our experiments, since the codes under consideration have short length and are also small in size, we perform Brute-force ML decoding in (5) to recover the secret bits. For decoding conventional codes, (5) reduces to the special case $|\mathcal{C}_j| = 1, \forall j$. We repeat this decoding procedure for all the codewords in the frame. After the decoding operation, the decoded secret bits from all the frames are collected to reconstruct the *cameraman* image at Eve. Subsequently, Bit Error Rate (BER) is computed by counting the number of bit-positions in which the reconstructed image differs from the original one.

As highlighted earlier, we fix the transmitter USRP position and then vary the receiver USRP position at 5 different locations, referred to as Placement 1, 2, 3, 4 and 5 (in the order of increasing distance). In Fig. 8, 9 and 10, we plot the received symbols $\{r\}$ (available at the input

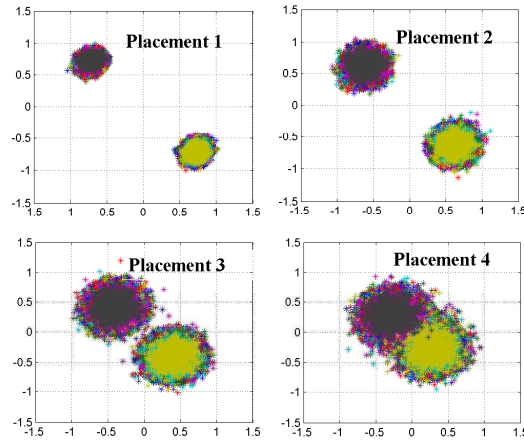


Fig. 8. The cloud of received points at different placements for conventional coding. The underlying constellation is $\{0, 1\}$, which is shifted and then rotated by -45 degrees before transmission.

of the data decoding block in Fig. 7) when symbols from the constellation $\{0, 1\}$, $\{0, 1, 2, 3\}$ and $\{0, 1, 2, \dots, 7\}$ are transmitted as shown in (7). Fig. 9 highlights that for Placement 1, the SNR at Eve is too high to cause degradation in the error performance with both conventional encoding and coset encoding with 1 bit confusion. However, for the same placement, coset encoding with 2 bits confusion can potentially introduce errors since the decision regions overlap. Similarly, for other placements (which corresponds to lower SNR values), it can be seen that coset encoding can potentially result in more errors for Eve.

For the four placements, we compute the corresponding baseband SNR values by transmitting unit energy training sequences. The received symbols are used to compute the SNR as $\frac{\mathbb{E}[|\hat{h}_E|^2]}{\mathbb{E}[|r|^2] - \mathbb{E}[|\hat{h}_E|^2]}$, where $\mathbb{E}[|\hat{h}_E|^2]$ indicates the average signal power and $\mathbb{E}[|r|^2] - \mathbb{E}[|\hat{h}_E|^2]$ is indicative of the average noise power. The measured SNR values at different frames are plotted in Fig. 11, which shows that the four placements correspond to the average SNR values of 20.6, 15, 9 and 4.5 dB, respectively.

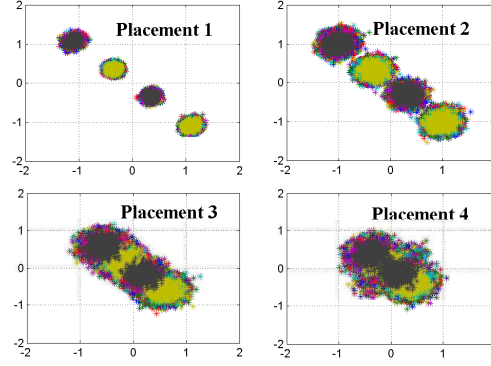


Fig. 9. The cloud of received points at different placements for coset encoding with 1 bit confusion. The underlying constellation is $\{0, 1, 2, 3\}$, which is shifted and then rotated by -45 degrees before transmission.

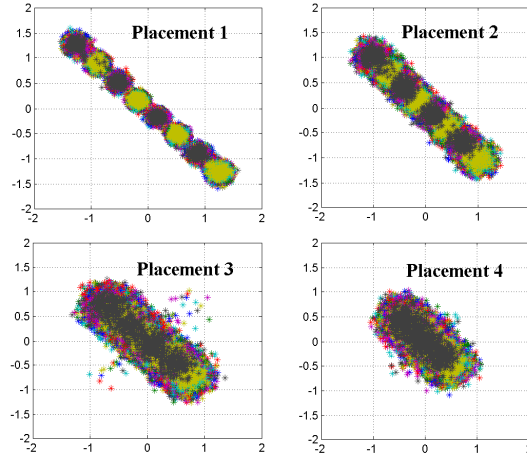


Fig. 10. The cloud of received points at different placements for coset encoding with 2 bits confusion. The underlying constellation is $\{0, 1, 2, \dots, 7\}$, which is shifted and then rotated by -45 degrees before transmission.

IV. IMPACT OF COSET CODING ON THE ERROR PERFORMANCE AT EVE

The signal transmitted from Alice to Bob is intercepted by Eve, after which it is appropriately sampled and then forwarded to a digital signal processing block to recover the image. Eve is assumed to know everything: the frame structure, modulation scheme, number of bits of confusion, and also the image size. Using the pilot symbols, Eve estimates the beginning of

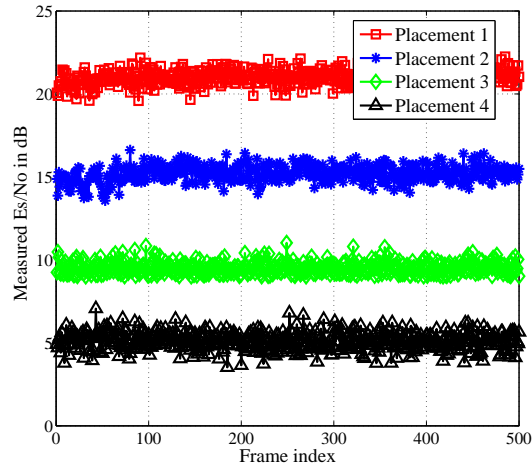


Fig. 11. Measured baseband SNR values at four different placements of the receive USRP. The estimated channel gain and the baseband received symbols of each frame are used to measure the SNR values.



Fig. 12. Reconstructed images at Eve in Placement 4. From left to right, (a) conventional encoding at Alice, (b) wiretap coding at Alice with one bit confusion, and (c) wiretap coding at Alice with two bits confusion.

every frame from the sequence of received symbols and decodes the information bits. For the decoding step, the method employed is either conventional or coset based, depending on the encoding method at Alice (which is presumed known at Eve).

We have conducted the experiments using wiretap codes over \mathbb{Z} with three different encoding schemes: (a) conventional encoding, (b) coset coding with one bit confusion, and (c) coset coding with two bits confusion. The schemes in (a) and (c) are the same as in Section II-B, however,

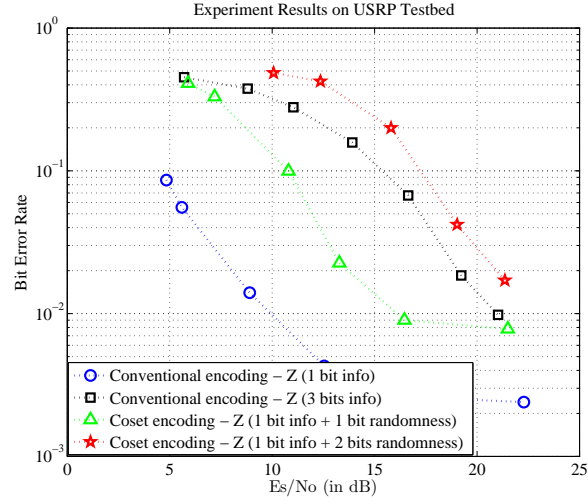


Fig. 13. Performance comparison between coset and conventional encoding schemes in \mathbb{Z} obtained from the reconstructed images at Eve. The above plots quantify the degradation in the reconstructed image as depicted in Fig. 12.

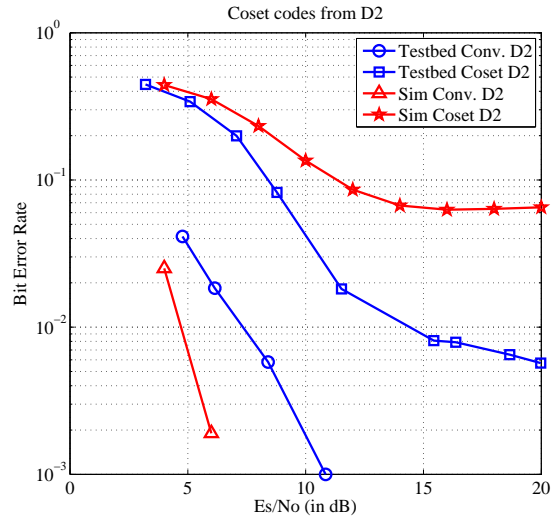


Fig. 14. Performance comparison between coset and conventional encoding schemes in D_2 obtained from experiments on testbed and computer simulations. Both experiments show that coset encoding degrades the error performance at Eve more than conventional encoding.

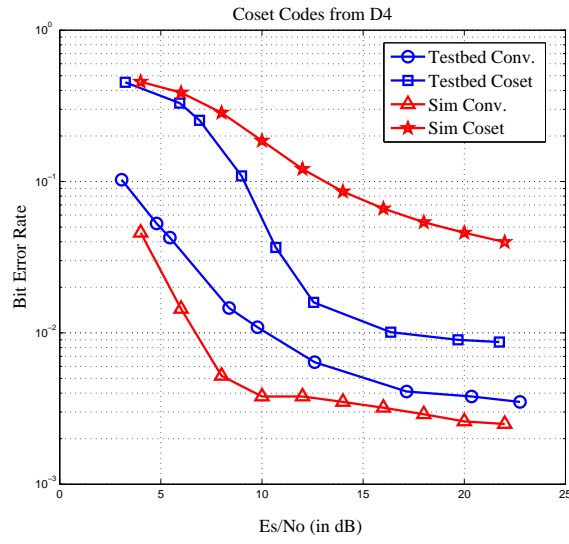


Fig. 15. Performance comparison between coset and conventional encoding schemes in D_4 obtained from experiments on testbed and computer simulations. Both experiments show that coset encoding degrades the error performance at Eve more than conventional encoding.

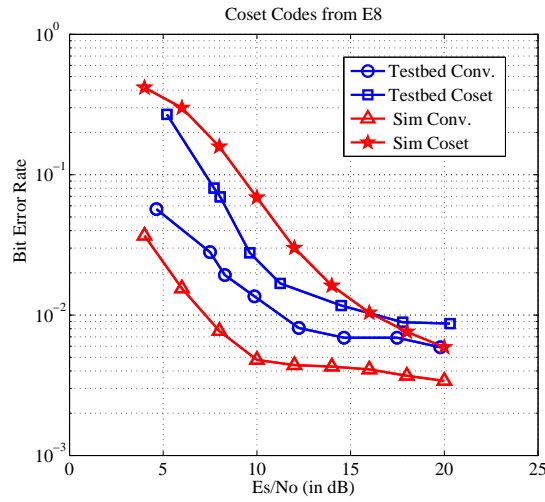


Fig. 16. Performance comparison between coset and conventional encoding schemes in E_8 obtained from experiments on testbed and computer simulations. Both experiments show that coset encoding degrades the error performance at Eve more than conventional encoding.

the one in (b) is different from (c) as it chooses one bit of randomness instead of two. The reconstructed images at Eve for these cases are displayed in Fig. 12. From Fig. 12, it is clear that Eve is able to recover most parts of the image with conventional coding. Although Eve's channel is noisier than that of Bob (by the virtue of longer distance), conventional coding is unable to introduce confusion for Eve at that position. However, it can be seen that coset coding with one bit confusion results in a more distorted image at Eve when compared to conventional coding. Finally, coset encoding with two bits confusion seems to be the best choice for secrecy at Placement 4 as no part of the image is visible. Meanwhile, Bob can correctly recover the image since he is at a distance much closer to Alice, thanks to which, coset coding with two bits confusion does not lead to erroneous reconstruction of the image. In summary, with the knowledge of Eve's distance, Alice is able to decide on the required number of confusion to maintain secrecy. The same behavior is quantified in Fig. 13, which shows the variation of BER for the above three schemes.

Other than using basic coset coding over \mathbb{Z} ($L = 1$), we also demonstrate the effect of higher dimensional coset lattice codes from D_2 ($L = 2$), D_4 ($L = 4$), and E_8 ($L = 8$), by using them to transmit the *cameraman image* between the USRP devices.

A. Coset Codes over Lattices D_2 , D_4 and E_8

For the experiments with $L = 2$, we have carved a lattice code from Construction A of D_2 given by

$$D_2 = 2\mathbb{Z}^2 + C = (2\mathbb{Z}^2 + (0, 0)) \cup (2\mathbb{Z}^2 + (1, 1)).$$

where $C = \{(0, 0), (1, 1)\}$ is the repetition code. For conventional lattice coding, one bit of secret is transmitted through the codewords of the repetition code. However, for coset lattice code, we introduce some randomness by choosing non-zero values from $2\mathbb{Z}^2$ in Construction A, i.e., we choose $\{(0, 0), (0, 1), (1, 0), (1, 1)\} \subset \mathbb{Z}^2$, in order to introduce 2 bits of randomness per codeword. Therefore, under coset coding, the transmitted points (before scaling and normalization)

take values from the set

$$\{(0, 2), (2, 0), (2, 2), (0, 0)\} + \{(0, 0), (1, 1)\},$$

to carry 2 bits of confusion and 1 bit of secret. Here $+$ is used to denote the direct sum of two sets. From the notations of Section II-C, the above wiretap lattice code can be written as

$$\mathcal{C} = \mathcal{C}_0 \cup \mathcal{C}_1,$$

where $\mathcal{C}_0 = \{(0, 2), (2, 0), (2, 2), (0, 0)\}$ and $\mathcal{C}_1 = \{(1, 3), (3, 1), (3, 3), (1, 1)\}$.

Similarly, lattice codes from D_4 given by

$$D_4 = 2\mathbb{Z}^4 + \mathcal{RM}(1, 2),$$

are also employed in our experiments. Here, $\mathcal{RM}(1, 2) = (n = 4, k = 3, d = 2)$ is the Reed-Muller code of length 4 and dimension 3. For this case, conventional lattice encoding will map 3 secret bits to the codewords of $\mathcal{RM}(1, 2)$, while in coset encoding, in addition to the 3 secret bits, some random bits are also mapped from the free part of Construction A, i.e., by forcing $\{0, 1\}^4 \subset \mathbb{Z}^4$. Thus, with coset encoding, 4 bits of randomness are transmitted with 3 bits of secret. Finally, lattice codes from E_8 given by

$$E_8 = 2\mathbb{Z}^8 + \mathcal{RM}(1, 3),$$

are also employed in our experiments. Here, $\mathcal{RM}(1, 3) = (n = 8, k = 4, d = 4)$ is the Reed-Muller code of length 8 and dimension 4. For this case, conventional lattice encoding will map 4 secret bits to the codewords of $\mathcal{RM}(1, 3)$, while in coset encoding, in addition to the 4 secret bits, some random bits are also mapped from the free part of Construction A, i.e., by forcing $\{0, 1\}^8 \subset \mathbb{Z}^8$. Thus, with coset encoding, 8 bits of randomness is transmitted with 4 bits of secret.

The performance comparison between higher-dimensional lattice coset codes and the corresponding conventional lattice codes are presented in Fig. 14 (for D_2), Fig. 15 (for D_4) and Fig.

16 (for E_8), which show that coset encoding offers degraded performance at Eve than that offered by conventional encoding schemes. From Fig. 14, we observe that for the location corresponding to 4 dB, coset encoding provides BER of 0.5 at Eve, whereas conventional encoding offers BER smaller than 10%. For the rest of the positions (equivalently higher SNR values), Eve gets partial knowledge of the secret even with coset encoding scheme. Therefore, the plots suggests that if Alice has to provide close to 0.5 BER for other locations, she might have to increase the number of random bits by ensuring that the error performance at Bob does not degrade.

B. Performance Comparison from Computer Simulations

Along with the results extracted from the testbed, we also present results obtained from computer simulations in Fig. 14 to Fig. 16 (legends in red), which echo similar observations made from the testbed results. Note that the BER behaviours from the simulations are substantially different from that of the testbed although they too emphasize that coset encoding provides higher confusion than conventional encoding. This difference is attributed to the facts that (i) computer simulations were obtained by simulating an AWGN channel with SNR values corresponding to that of the average SNR measured over all frames, whereas in the testbed experiments, each frame experiences a different SNR level as shown in Fig. 11, and (ii) the entire chain of receiver-side operations pointed in Fig. 7 is replaced by an additive noise channel in the simulations thereby resulting in different channel model than that in the testbed.

V. DISCUSSION

In this paper, we have demonstrated the impact of lattice coset codes for introducing confusion at an eavesdropper that experiences a channel that is noisier than that of Bob. In the experiments, we have incorporated the assumption of degradedness by placing Eve farther away from Alice than Bob. As a natural consequence of farther distance, error performance at Eve is worse than that at Bob. In addition, we have shown that adding randomness at the transmitter can further

degrade the error performance at Eve. However, additional randomness is carefully added so as not to deteriorate the performance of Bob. One of the main assumptions of this work is that Alice knows the location of Eve (or the equivalent signal-to-noise ratio), and hence, she can decide on the number of random bits. A strong defense to this assumption is the scenario wherein there is physical restriction imposed on the proximity of Eve. This work can be further extended in the following directions: (i) We have conducted experiments using single antenna devices. Advanced physical-layer techniques can be tested on similar testbeds with multiple antenna devices. (ii) We have assumed that the location of the eavesdropper is known to Alice (so as to decide on the amount of randomness to be added). A challenging direction for future work is to detect the presence of an eavesdropper based on the local oscillator leakage [13], and then estimate its distance to decide on the quantum of randomness. Alternatively, bits could be encoded in a hierarchical manner, providing more protection to the most significant ones.

REFERENCES

- [1] Y. Liang, H. V. Poor and S. Shamai (Shitz), “Information Theoretic Security”, Foundations and Trends in Communications and Information Theory: Vol. 5: No. 45, 2009.
- [2] F. Lin and F. Oggier, “Coding for Wiretap Channels”, in “Physical Layer Security in Wireless Communications”, X. Zhou, L. Song, Y. Zhang, CRC Press, 2013.
- [3] D. Kline, J. Ha, S. McLaughlin, J. Barros, and B.-J. Kwak, “LDPC codes for the Gaussian wiretap channel,” *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 532–540, Sep. 2011.
- [4] M. Baldi, M. Bianchi, and F. Chiaraluce, “Coding with scrambling, concatenation, and HARQ for the AWGN wire-tap channel: A security gap analysis,” *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 883–894, Jun. 2012.
- [5] Y. Zhang, A. Liu, C. Gong, G. Yang, and S. Yang, “Polar-LDPC concatenated coding for the AWGN wiretap channel,” *IEEE Commun. Lett.*, vol. 18, no. 10, pp. 1683–1686, Oct. 2014.
- [6] A. J. Pierrot, R. A. Chou, M. R. Bloch, “The Effect of Eavesdroppers Statistics in Experimental Wireless Secret-Key Generation”, <http://arxiv.org/pdf/1312.3304.pdf>
- [7] J. H. Conway, N. J. A. Sloane, “Sphere Packings, Lattices and Groups”, 3rd edition, Springer.
- [8] C. Ling, L. Luzzi, J.-C. Belfiore, and D. Stehlé, “Semantically Secure Lattice Codes for the Gaussian Wiretap Channel”, *IEEE Transactions On Information Theory*, Vol. 60, no 10, October 2014.

- [9] J. Lu, J. Harshan, F. Oggier, "A USRP Implementation of Wiretap Lattice Codes," *Information Theory Workshop (ITW)*, Tasmania, 2014.
- [10] <https://sites.google.com/site/usrplattice/>
- [11] R. H. Barker "Group Synchronizing of Binary Digital Sequences," *Communication Theory*. London: Butterworth. pp. 273287, 1953.
- [12] http://www.mathworks.com/help/shared_sdr_sdru/examples/
- [13] B. Wild and K. Ramchandran, "Detecting primary receivers for cognitive radio applications," *IEEE DySPAN, 2005*, Baltimore, MD, USA, 2005, pp. 124-130.